~~SECRET PENDING CLASSIFICATION REVIEW~~

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

SECRET PENDING CLASSIFICATION REVIEW

S3 17 Cr. 548 (JMF)

GOVERNMENT'S OMNIBUS MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S MOTIONS

DAMIAN WILLIANS
United States Attorney
Southern District of New York

David W. Denton, Jr.
Michael D. Lockard
Assistant United States Attorneys,
Of counsel

~~SECRET PENDING CLASSIFICATION REVIEW~~

TABLE OF CONTENTS

~~SECRET PENDING CLASSIFICATION REVIEW~~

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum of law in opposition to the omnibus motion dated January 28, 2022 (the "Motion" or "Mot.") filed by the defendant, Joshua Adam Schulte (the defendant or "Schulte") seeking to (1) suppress evidence from electronic accounts searches; (2) sever certain counts relating to the defendant's illegal transmission and attempted transmission of national defense information from the Metropolitan Correctional Center ("MCC") from the other counts; (3) preclude expert testimony based on purported discovery violations; (4) compel discovery; and (5) suppress documents obtained from his cell at the MCC pursuant to search warrants.

As set forth below, the defendant has previously sought the relief that he seeks again in the Motion, based largely on the same arguments or variations thereof, and the Court has denied those requests.

- By Order dated October 31, 2019 (D.E. 168) (the "Suppression Decision"), the Court denied the defendant's motion to suppress, *inter alia*, the results of the searches of the electronic accounts.
- By Order dated September 26, 2019 (D.E. 147) (the "Severance Decision"), the Court denied the defendant's motion to sever counts related to his MCC conduct from the other charged counts in an underlying indictment.
- By Order dated September 23, 2021 (D.E. 514) (the "NetApp Discovery Decision"), the Court denied the defendant's motion to compel the production of the same discovery that, the defendant now claims, warrants precluding the Government's expert witnesses.
- In the NetApp Decision and additional Orders dated July 22, 2019 (D.E. 124) (the "Section 4 Decision") and December 13, 2019 (classified) (the "Section 6(a) Decision"), the Court denied the defendant's motions to compel certain classified discovery, and the Government has produced the other relevant discovery the defendant seeks.
- By Orders dated October 18, 2019 (D.E. 159) (the "MCC Suppression Decision") and January 30, 2020 (D.E. 288) (the "Cell Documents Decision"), the Court denied the defendant's motions to suppress the results of searches of the MCC and to exclude particular documents obtained from his cell.

The defendant's Motion provides no compelling reasons for the Court to reconsider these prior Orders and, indeed, the Motion largely repeats the same arguments the Court has already rejected and variations thereof. Even if the defendant's arguments were considered anew, they are without merit, and the Motion should be denied in its entirety.

BACKGROUND

As the Court is aware, the charges in this case stem from an investigation into WikiLeaks's disclosure of certain classified information stolen from the Central Intelligence Agency ("CIA"). Between March 7 and November 17, 2017, WikiLeaks made 26 separate disclosures of classified CIA information (together, the "Leaks"). The Leaks contained, among other things, highly sensitive CIA information including detailed descriptions of certain tools used by CIA operators. The Leaks' impact on the CIA's intelligence gathering activities and the national security of the United States was catastrophic.

I. The Defendant's Theft of National Defense Information from the CIA and Transmission of the Stolen Information to WikiLeaks

The defendant was a CIA employee in the Engineering and Development Group ("EDG"), where he and his former colleagues developed cyber tools that were developed and stored on a closed, classified computer network called DevLAN. In late 2015 and early 2016, Schulte became disaffected and began misusing his system administrator privileges, on one occasion restoring his previously revoked system administrator privileges to a particular project without authorization and on another occasion revoking his colleagues' system administrator privileges to another project without authorization. Following the defendant's abuses of his system administrator privileges (increased access to the network to modify the network) in April 2016, system administrator protocols for DevLAN were revamped and the defendant's administrator access to the network used to develop cyber tools was eliminated. The defendant hid from his supervisors,

however, that he retained an access key to the physical server where the development tools were stored. D.E. 410 at 4-9.

On April 20, 2016, the defendant learned that the suite of software and libraries used by the group for cyber tool development would soon be moved to a different physical server, to which he did not have access. That evening, when he was the last person in the office, the defendant used his access key to the server to steal highly classified data from the CIA cyber tool arsenal before his access was permanently blocked. The defendant used his server access to create a "snapshot" of the server as it existed at that time and then reverted the network to a saved state that existed on April 16, 2016—before his network administrator privileges had been revoked. The defendant used his restored system administrator access to copy backup files from the network (the "Stolen Information"), then reversed the reversion so that the network was back to its April 20, 2016 state. The defendant then deleted the snapshot of the system he had created as well as several thousand log files on the server in an effort to conceal his actions on the network. *Id.* at 10-13. In the approximately two weeks following his theft of the Stolen Information, the defendant downloaded a program recommended by WikiLeaks for the transmission of stolen data, researched data-transfer and -deletion techniques, transferred a large volume of data from his home computer, and, on May 5, 2016, reformatted his entire home computer hard drive, erasing all data from his computer and making it unretrievable through forensic examination. *Id.* at 13-14.

II. The Defendant's Arrest, Bail, and Bail Revocation

The defendant was arrested on August 24, 2017, based on a criminal Complaint alleging child pornography crimes, and ordered detained. D.E. 4. An indictment was returned on September 6, 2017. D.E. 6. At his arraignment, the defendant was released on conditions. D.E. 8. On September 18, 2017, the Court entered a discovery protective order D.E. 11 (the "Protective Order") prohibiting disclosure of protected materials outside the defense team. On August 16,

2018, the Court entered the Classified Information Protective Order that, *inter alia*, prohibits the defendant and defense counsel from disclosing classified information to anyone except the Court and government personnel holding the appropriate clearances and a need-to-know. D.E. 61 at 5. On December 14, 2017, following his arrest on state sexual assault charges in Virginia, the defendant's bail was revoked. D.E. 22; *see also* D.E. 26 & 33.

On June 18, 2018, based on the information gathered as part of the investigation, the defendant was charged in a thirteen-count Indictment with espionage and other offenses related to the Leaks, as well as child pornography and copyright offenses for which the defendant previously was arrested. D.E. 47 (First Superseding Indictment).

III. The Defendant's Disclosure and Attempted Disclosure of Classified Information from the MCC

Following the defendant's initial arrest, he engaged in a campaign to publicly promote false claims of having been framed by the Federal Bureau of Investigation ("FBI") and CIA. In May 2018, two newspapers published articles referencing search warrants produced in discovery pursuant to the Protective Order (the "Protected Search Warrants"). Trial Tr. 2467-68, GX829. The Court held a hearing at which the Court reiterated the requirements of the Protective Order and confirmed that the defendant understood its terms. *Id.* at 7-8.

In July 2018, the defendant's relatives posted to Facebook drafts of "articles" the defendant had written, but failed to post the versions that Schulte wanted publicized. GX801, 806, 809. The defendant's "articles" were part of his self-declared "information war" against the United States. GX809. In approximately August 2018, the defendant and another inmate obtained access to contraband cellphones (the "Contraband Cellphones") GX821, 5003, which the defendant used to create Facebook, Twitter, and email accounts, including encrypted and anonymized email accounts (the "Encrypted Accounts"). GX809, 822, 1303-2. The defendant intended to publish his "articles"

through these accounts, as well as purported statements by CIA and FBI employees claiming that the defendant was framed. GX809. The defendant's draft posts included classified information about CIA cyber techniques and a particular CIA cyber tool called "Bartender." *Id.*

The defendant, pretending to be someone else, began communicating with one of the authors of the May 2018 articles in August 2018 using the Encrypted Accounts. GX809, 1303-2, 1303-11. The defendant offered to provide the reporter with nonpublic information, *id.*, and in September 2018 emailed the reporter information from the Protected Search Warrants, including an attempted refutation of statements in the supporting affidavit that included classified information. GX1303-34. Before the defendant could disclose additional classified information, the FBI disrupted the defendant's plans by executing searches, pursuant to search warrants, of the MCC and the defendant's electronic accounts. Trial Tr. 2471, 2644.

Based on this conduct, on October 31, 2018, the grand jury returned a second superseding indictment charging him with one additional count of unlawfully disclosing and attempting to disclose classified information and one count of contempt of court. D.E. 68 (Second Superseding Indictment). The Attorney General also authorized Special Administrative Measures ("SAMs"), 28 C.F.R. Part 501. D.E. 127 at 3-4. Pursuant to the SAMs, the defendant is in a Special Housing Unit and has restricted and monitored communications. *Id.* at 4-5.

IV. The Prior Trial

On February 2, 2020, trial began as to the eleven national security-related counts in the Second Superseding Indictment. On March 9, 2020, a jury found the defendant guilty of making false statements to law enforcement, 18 U.S.C. § 1001, and contempt of court, 18 U.S.C. § 401(3). The jury did not reach a unanimous verdict on the remaining counts and the Court granted the defendant's motion for a mistrial as to those counts.

On June 8, 2020, a third superseding indictment was filed, D.E. 405 (Third Superseding Indictment), containing nine counts based on the same conduct at issue during the February 2020 trial, namely, the defendant's theft and transmission of CIA information, his deletion of data on CIA computer systems while committing that theft, his obstruction of the resulting investigation, and his transmission and attempted transmission of classified information while detained.

DISCUSSION

I. The Defendant's Motion to Suppress Electronic Searches Should Be Denied

A. Background

1. The Search of the Defendant's Residence

Within a week of the first of the Leaks being published on the internet by WikiLeaks on March 7, 2017, law enforcement identified the defendant as a likely suspect. Based on preliminary and ongoing analysis of Stolen Information contained in the Leak, the FBI had identified the CIA group from which the stolen data came; believed that the Leak came from daily backup files of that group's computer systems; and believed that the stolen data was from a backup created in early March 2016. *See* Ex. A ¶¶ 7-10. The defendant was one of a small number of people having system administrator access to the relevant backup files around the likely time of the theft; he possessed the skills and knowledge that likely would have been required to steal and disseminate the data; and his name—unlike the names or pseudonyms of other CIA personnel with access to the backup data—was not included in the initial Leaks. *Id.* ¶¶ 11-13.

The FBI also had learned that, in early April 2016, the defendant had restored his own previously revoked administrator privileges without authorization, *id.* ¶¶ 14-15; and that, in May 2016, the defendant had revoked other CIA personnel's administrator privileges without authorization. *Id.* ¶ 15. The FBI had also learned of a contentious personnel dispute between the defendant and a former colleague, and the defendant's disagreement with how the dispute was

resolved. *Id.* ¶¶ 17-18. The defendant resigned from the CIA in November 2016. *Id.* ¶ 19. In connection with his resignation, the defendant claimed to have raised network security concerns with various CIA supervisors and claimed that lax network security made it "easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA group computer code] in its entirety to the [public] internet." *Id.* ¶ 20. On his last day at the CIA, the defendant carried out of the office a printed copy of an email that he had written and marked "unclassified" that, in fact, contained classified information. *Id.* After the first of the Leaks was published by WikiLeaks on March 7, 2017, the defendant reached out to several of his former colleagues in an attempt to learn the status of the investigation into the Leaks and the extent to which the defendant was a suspect. *Id.* ¶ 20.[1] The FBI also learned that the defendant had international travel planned on March 15, 2017. *Id.* ¶ 21.

On March 13, 2017, the Honorable Barbara Moses, United States Magistrate Judge, issued a warrant authorizing the covert search of the defendant's apartment in Manhattan, New York, including electronic devices. *See* Ex. A-1. The warrant was based on the affidavit of FBI Special Agent Jeff D. Donaldson. Ex. A. Based on the covert warrant, FBI personnel entered the defendant's apartment, where they found a desktop computer, a server rack, at least five external hard drives, and multiple other electronic devices, the imaging of which would have been extremely time-consuming and likely would have led to the search being detected or interrupted by the defendant. *See* Ex B ¶ 8. In the early hours of March 14, 2017, Judge Moses issued a second warrant authorizing the overt search of the apartment (Ex. B-1), which was executed on or about March 15, 2017. D.E. 525 at 2-3.

[1] On September 18, 2018, the Government sent a letter to defense counsel describing additional information, developed through the ongoing investigation after March 13, 2017, relevant to some of the statements in the March 13 and 14, 2017 affidavits. (D.E. 111 Ex. F).

2. The Searches of the Electronic Accounts

Also in the early hours of March 14, 2017, Judge Moses issued warrants to search accounts associated with the defendant hosted by Google, Inc. and Github.com, and a Reddit account. *See* Ex. C-1 (the "Electronic Accounts Warrants"). The warrants were based on the affidavit of Special Agent Donaldson, *See* Ex. C (the "Affidavit"), which recited substantially the same facts in support of probable cause to believe that the subject offense had been committed and that the defendant had committed them as in the application for the covert warrant. *Id.* ¶¶ 13-26.

The Affidavit further described that the defendant used services associated with his Google account and a telephone number to which his Google account was registered to communicate with former colleagues about the Leaks and in the immediate aftermath of the Leaks, both by voice call and by text communication. *Id.* ¶ 27. The defendant's Google account included services likely to contain evidence of the subject offenses. *Id.* ¶¶ 27(d) & 5.

The Affidavit also described that Reddit message thread that was opened on the day of the Leaks that discussed the Leaks, identified the defendant and one of his usernames ("pedbsktbll"), linked to information from the defendant's GitHub account, and asked, "What about this guy[?]" *Id.* ¶ 28(a)-(c). The linked GitHub account contained computer code and references to computer applications referenced in the Leaks. *Id.* ¶ 29. The Affidavit described the defendant's proficiency in internet-based computing services; that internet-based services are often used by offenders to communicate with co-conspirators and to transmit and store stolen information; WikiLeaks is an internet-based publication; and individuals submit information to WikiLeaks using, among other means, internet-based computing platforms. *Id.* ¶ 30.

A review of the contents of the defendant's Google account pursuant to the Electronic Accounts Warrants showed that, among other things, in April and May 2016, the defendant conducted searches and visited websites relating to large-file copying utilities, portable electronic

media copying speeds, using system administrator privileges to review restricted files and to restrict other administrators' ability to view aspects of the network, the permanent deletion of files from computer storage media, large-file transferring tools, and anonymous internet data-transfer tools, among other things. Ex. D ¶¶ 27-29. The defendant also conducted numerous searches relating to WikiLeaks between approximately August 2016 and March 2017, including searches relating to data transfer platforms recommended by WikiLeaks to submit stolen data. *Id.* ¶¶ 31-32.

3. The Defendant's Prior Motion to Suppress the Residence Search and the Electronic Accounts Searches

On July 3, 2019, the defendant, through counsel, filed a motion to suppress the results of the covert apartment search, the overt apartment search, and the electronic accounts searches. D.E. 109. The defendant argued, *inter alia*, that the affidavits in support of the searches contained reckless or intentional misstatements of fact or omissions of fact under *Franks v. Delaware*, 438 U.S. 154 (1978), *see id.* at 15-21; and that the warrants were overbroad and insufficiently particularized, amounting to general warrants. *Id.* at 40-45. With respect to particularity, the defendant argued that the warrants, including the Electronic Accounts Warrants, "authorized the government to seize and search virtually everything they could find relating to Mr. Schulte," *id.* at 43; "were impermissibly broad because they described generic types of data without any reference to the suspected criminal conduct," *id.* at 44; "lacked any temporal limitation," *id.*; and "'lacked the requisite specificity to allow for a tailored search of [the defendant's] electronic media' and 'fail[ed] to link the items to be searched and seized to suspected criminal activity,'" *id.* at 45 (quoting *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010) (alterations in original)).

By order dated October 31, 2019, the Court denied the defendant's suppression motion in its entirety. *See* Suppression Decision. The Court held the affidavit in support of the March 13,

2017 covert warrant established probable cause for the search, even omitting the factual statements challenged by the defendant. *Id.* at 2 and 9-13.

> Excluding the challenged statements, the affidavit provides the following which is sufficient to determine that there is a "fair probability that contraband or evidence of a crime" would be found in Schulte's apartment on his electronic devices, Schulte: (1) had the necessary skills and unique access to the stolen information and LAN network, (2) had a deep understanding of the relevant CIA computer systems and information exposed by the Wikileaks, (3) had a motive to harm the CIA because he was angry that the CIA did not take his complaints seriously, (4) had threated to go public previously, (5) had secured unauthorized access to Classified Information in violation of CIA directives, (6) had drafted an email warning CIA management about security vulnerabilities that could expose information from the LAN that eventually was exposed by Wikileaks, and (7) demonstrated a guilty conscience. These facts support a conclusion that Schulte had both a motive and opportunity to take the classified CIA information. Further, the nature of the LAN network—an isolated network that cannot be accessed from the public internet—strongly suggests that the theft of classified information was an inside job and the information was believed to have been stolen using portable media given the substantial amount of data published. Finally, the affidavit contained an extensive discussion of the modus operandi of those who engage in espionage, including how such files are transferred, stored, and leave a lasting digital footprint. Taken together, these facts support a finding of probable cause to issue a search warrant.

Id. at 10-11.

The Court also rejected the defendant's arguments that the affidavits in support of the warrants relied on stale evidence that did not establish probable cause to believe that evidence of the offenses would be found in the defendant's apartment, and on his electronic devices and media, at the time of the searches in March 2017. "Where, as here, the crime involves leaking classified information and the leak was published one week before the warrant issued, the basis for the search is not automatically stale where an affidavit alleges such information was gathered (or stolen) a year earlier. The nature of espionage provides that conduct may be ongoing because gathering or stealing classified information could have occurred long before the actual transmission. . . . [T]he

affidavit provided facts suggesting ongoing publishing of classified CIA information by Wikileaks—*i.e.*, the March 7 Leak constituted the 'first full part' of a series. Thus, the FBI reasonably could have inferred that Schulte had transmitted classified information from his New York City apartment shortly before the initial Wikileaks publication and could have reasonably inferred that transmission was ongoing." *Id.* at 12-13.

4. The Defendant's New Motion to Suppress the Electronic Account Searches

In his new Motion, the defendant acknowledges that he "previously filed a motion to suppress evidence seized from the March 13, 2017 search of his apartment on July 3, 2018" Mot. 1, and argues that the Motion "challenges the constitutionality of the Google, Reddit, and Github warrants that were issued on March 14, 2017." The Motion seeks to challenge "whether the warrant establishes the minimal factual nexus between the alleged offense and the online accounts to search; and whether the warrants were sufficiently particular." *Id.*

B. Relevant Law

1. Reconsideration

"Reconsideration of a court's previous order is an extraordinary remedy to be employed sparingly in the interests of finality and conservation of scarce judicial resources," *United States v. Almonte*, No. 14 Cr. 86 (KPF), 2014 WL 3702598, at *1 (S.D.N.Y. July 24, 2014) (internal quotation marks omitted); and it is "not intended as a vehicle for relitigating old issues, presenting the case under new theories or otherwise taking a second bite at the apple." *United States v. Nero*, No. 13 Cr. 271 (LTS), 2021 WL 1534392, at *1 (S.D.N.Y. Apr. 19, 2021) (internal quotation marks and alteration omitted). "While the Federal Rules of Criminal Procedure do not provide for reconsideration motions, such motions are tacitly accepted in criminal cases in this District by virtue of Local Crim. R. 49.1(d), which requires a movant to submit a 'memorandum setting forth

concisely the matters or controlling decisions which counsel believes the Court has overlooked' within 'fourteen (14) days after the Court's determination of the original motion.' Courts generally supplement Local Criminal Rule 49.1(d) with the standard for civil reconsideration motions under Local Civ. R. 6.3." *United States v. Baldeo*, No. S1 13 Cr. 125 (PAC), 2015 WL 252414, at *1 (S.D.N.Y. Jan. 20, 2015), *aff'd*, 615 F. App'x 26 (2d Cir. 2015). The untimeliness of a defendant's motion "is itself a sufficient basis for denial," although "courts retain the discretion to excuse an untimely filing." *United States v. Lisi*, No. 15 Cr. 457 (KPF), 2020 WL 1331955, at *1 (S.D.N.Y. Mar. 23, 2020).

"The standard governing reconsideration motions is strict, and reconsideration will generally be denied unless the moving party can point to controlling decisions or data that the court overlooked—matters, in other words, that might reasonably be expected to alter the conclusion reached by the court." *United States v. Donziger*, No. 19 Cr. 561 (LAP), 2021 WL 1845104, at *3 (S.D.N.Y. May 7, 2021). "Compelling reasons for granting a motion for reconsideration are limited to an intervening change of controlling law, the availability of new evidence, or the need to correct a clear error or prevent manifest injustice." *United States v. Bush*, No. 18 Cr. 907 (PAC), 2021 WL 371782, at *1 (S.D.N.Y. Feb. 3, 2021) (cleaned up). Motions for reconsideration "may not advance new facts, issues or arguments not previously presented to the Court, nor may [they] be used as vehicle[s] for relitigating issues already decided by the Court." *Baldeo*, 2015 WL 252414, at *1 (quoting *Davidson v. Scully*, 172 F. Supp. 2d 458, 461 (S.D.N.Y. 2001)). Thus, although ultimately "[t]he decision to grant or deny a motion for reconsideration is within the sound discretion of the district court," *Lisi*, 2020 WL 1331955, at *1, "[w]here a motion restates arguments already presented or attempts to advance new facts . . . the motion for reconsideration

must be denied." *United States v. Alvarez-Estevez*, No. 13 Cr. 380 (JFK), 2014 WL 12681364, at *1 (S.D.N.Y. Nov. 6, 2014).

2. Search Warrants

Consistent with the Fourth Amendment, a search warrant must "describe with particularity the place to be searched and the persons or things to be seized." *United States v. Rosa*, 626 F.3d 56, 61 (2d Cir. 2010). In considering a request for a search warrant, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Such determinations must be approached in a practical way, *id.* at 231-32, because "probable cause is a flexible, common-sense standard," *Texas v. Brown*, 460 U.S. 730, 742 (1983). The warrant must be sufficiently particular in "specify[ing] the items to be seized by their relation to designated crimes," *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (cleaned up); but "courts may tolerate some ambiguity in the warrant so long as 'law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.'" *Id.* (quoting *United States v. Young*, 745 F.2d 733, 759 (2d Cir. 1984)).

Once a search warrant has issued, the issuing judge's "determination of probable cause should be paid great deference by reviewing courts." *Gates*, 462 U.S. at 236 (internal quotation marks omitted). "[A]fter-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review." *Id.* Thus, "'[a]lthough in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be

accorded to warrants.'" *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965)). "[S]o long as the magistrate had a 'substantial basis for . . . conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." *Gates*, 462 U.S. at 236 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)) (ellipsis and second alteration in original); *see also United States v. Singh*, 390 F.3d 168, 181 (2d Cir. 2004) ("In reviewing a magistrate's probable cause determination, we accord substantial deference to the magistrate's finding and limit our review 'to whether the issuing judicial officer had a substantial basis for the finding of probable cause.'" (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)).

Even if a warrant is defective, the seized evidence may still be admitted under certain circumstances, including the good faith exception. The Supreme Court, in *United States v. Leon*, 468 U.S. 897 (1984), held that the exclusionary rule "does not apply to evidence seized 'in objectively reasonable reliance on' a warrant issued by a detached and neutral magistrate judge, even where the warrant is subsequently deemed invalid." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008) (quoting *Leon*, 468 U.S. at 922). The Supreme Court has made clear that "the exclusionary rule is not an individual right and applies only where it results in appreciable deterrence." *Herring v. United States*, 555 U.S. 135, 141 (2009) (internal quotation marks and citations omitted). Thus the central question is "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n.23. If the reviewing court finds that the officer's reliance on the warrant was objectively reasonable, suppression is not warranted. *See id.* at 922; *Davis v. United States*, 564 U.S. 229, 238-39 (2011) ("*Leon* itself, for example, held that the exclusionary rule does not apply when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid."). To trigger

the exclusionary rule, law enforcement "conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144.

C. Argument

1. The Defendant's Motion Fails to Identify Controlling Decisions or Facts the Court Overlooked

The defendant's challenges to the March 14, 2017 warrants to search electronic accounts, D.E. 109 at 40-45, already has been rejected by the Court. *See* Suppression Decision. Though the Suppression Decision did not expressly address the defendant's challenges to the electronic accounts search, the Court "need not detail all of [its] reasons" and "any arguments [the party] made that were not expressly rejected in the Opinion and Order were rejected implicitly." *Ediagbonya v. United States*, No. 18 Civ. 3882 (VSB), 2021 WL 4226400, at *3 (S.D.N.Y. Sept. 15, 2021) (quoting *Dreni v. Printeron Am. Corp.*, No. 18 Civ. 12017 (MKV), 2021 WL 4066635, at *3 (S.D.N.Y. Sept. 3, 2021), and citing *Miller v. Met. Life Ins. Co.*, No. 17 Civ. 7284 (AT) (SN), 2018 WL 5993477, at *5 n.5 (S.D.N.Y. Nov. 15, 2018)).

The defendant's new motion to suppress the electronic account searches identifies no "intervening change of controlling law," no "availability of new evidence," and identifies no "clear error" in the Court's prior ruling. *Bush*, 2021 WL 371782, at *1. All of the facts cited in the Motion were known to the defendant at the time of his former counsel's motion, he repeats arguments that his former counsel made, *see* D.E. 109 at 40-45, and no law has changed that warrants revisiting the Court's denial of that former motion. Accordingly, the Court should not reconsider its order denying the defendant's prior motion to suppress evidence obtained from the electronic accounts searches.

2. The Defendant Disclaims Standing to Challenge the Search of the Reddit Account

The Affidavit did not allege that the subject Reddit account was the defendant's, *see* Ex. C ¶ 28, and the defendant affirmatively states that the account is not his. Mot. 6. The "capacity to claim the protection of the Fourth Amendment depends upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." *United States v. Watson*, 404 F.3d 163, 165 (2d Cir. 2005) (cleaned up). The defendant, accordingly, lacks standing to challenge the search of this account and his request to suppress evidence from the Reddit account should be denied for this additional and independent reason.

3. The Affidavit Establishes a Nexus Between the Electronic Accounts and Evidence of the Subject Offenses

Even addressing the merits of the defendant's new motion, his attempt to suppress the electronic accounts searches fails. The defendant's new motion does not contest probable cause that he committed the offenses of stealing and transmitting classified, national defense information from the CIA. Mot. 1-2. He argues that the Affidavit fails to establish a nexus between the subject offenses and the accounts to be searched, but his arguments omit portions of the Affidavit relevant to nexus; advance alternative, innocent interpretations of evidence; and levy speculative and unfounded attacks on the veracity of the Affidavit's allegations.

The defendant's principal argument in his Motion is that the Affidavit establishes probable cause that he committed the computer crimes and espionage offenses,[2] but not probable cause to

[2] The unauthorized possession and communication of national defense information to someone not entitled to received it, 18 U.S.C. § 793(d); the unlawful retention of national defense information, 18 U.S.C. § 793(e); exceeding authorized access to a computer to obtain national defense information with reason to believe it could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting it to a person not entitled to receive it, 18 U.S.C. § 1030(a)(1); and intentionally exceeding authorized access to a computer and

believe that evidence of the offenses would be found in the Google, GitHub, and Reddit accounts. Mot. 3-7. "A showing of nexus does not require direct evidence and may be based on reasonable inference from the facts presented based on common sense and experience." *Singh*, 390 F.3d at 182 (cleaned up). The defendant's argument rests on an incomplete and inaccurate reading of the Affidavit and an attempt to ignore reasonable inference and common sense.

The Affidavit describes a crime involving the transmission and dissemination of classified, national defense information over the internet: the Leaks were published by WikiLeaks on its website. Ex. C ¶ 13. The first potion of the Leaks was published on the internet on March 13, 2017, with the promise of more to come. *Id.* The defendant, in a draft resignation letter shared with a colleague in October 2016, claimed that sensitive CIA code could be downloaded from the CIA network and uploaded to the internet. *Id.* ¶ 25(a)(iv). WikiLeaks is an internet-based organization and receives information through internet-based computing platforms. *Id.* ¶ 30. Not only was there probable cause to believe that the defendant stole classified information as early as March 2016 and was discussing uploading stolen classified information to the internet in October 2016, but he also used services associated with his Google account to discuss the Leak with former colleagues from the CIA in March 2017 and to contact former colleagues in the time period immediately following the Leak. *Id.* These facts sufficiently establish probable cause to believe that the defendant's Google account would have evidence of the Subject Offenses, including (i) "[e]vidence relating to the participation in the Subject Offenses by users of the Target Accounts and others, including information relating to the unauthorized retention, gathering, and transmission of classified documents or materials; and the unauthorized removal and retention of

---

thereby obtaining information from a department or agency of the United States, 18 U.S.C. § 1030(a)(2)(B) (the "Subject Offenses"). (Ex. C ¶ 12).

classified documents and materials;" (ii) "correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials; and the unauthorized removal and retention of classified documents and materials;" and (iii) "[e]vidence concerning financial institutions and transactions used by the users of the [Google account] in furtherance of the Subject Offenses." *Id.* ¶ 33; *see also* Ex. C-1 at 3-4. The Affidavit also establishes probable cause that geolocation information relating to the time period of the Subject Offenses, evidence of the identity of the user(s) of the account, evidence of other computers or online accounts that may contain evidence relating to the Subject Offenses, and of passwords or other information needed to access such computers and accounts would be found in the Google account. *Id.*

The defendant's characterization of the probable cause to search his Google account as simply "that Mr. Schulte used his cellphone to contact former coworkers, with whom he remained friends after he left the CIA, [and] therefore Mr. Schulte must have used his cellphone and Google account to commit espionage" is wrong and ignores substantial evidence that internet-based accounts were used to commit the Subject Offenses and would contain evidence relating to the commission of the Subject Offenses. *See supra* 8, 17-18 & Ex C. The defendant's attempt to proffer innocent explanations for his conduct is also irrelevant—the Affidavit does not have to eliminate innocent interpretations in order to establish probable cause, *cf. Posner v. City of New York*, No. 11 Civ. 4859 (JMF), 2014 WL 185880, at *6 (S.D.N.Y. Jan. 16, 2014) ("The fact that Plaintiff has innocent explanations for the information that was known to Defendants, however, does not mean that they lacked probable cause; it merely means that she might have had viable arguments and defenses to the charges at trial."); and, in any event, the totality of the circumstances here established that the defendant's communications with his former colleagues "demonstrated a guilty conscience." Supp. Dec. at 10-11.

The defendant also attacks the affiant's training and experience, characterizing statements about the use of the internet and online accounts in furtherance of the Subject Offenses as "conclusory" and arguing that the affiant lied about having training and experience in espionage offenses. Mot. 7-10. The Affidavit, however, amply establishes the affiant's training and experience: Special Agent Donaldson has been employed by the FBI since 2010 and has worked in the field of counterintelligence since that time. Ex. C ¶ 1. At the time of the Affidavit, Special Agent Donaldson was assigned to a squad responsible for counterespionage matters. *Id.* He is familiar with the tactics, methods, and techniques of United States persons who misuse access to classified information through involvement in investigations involving espionage and the unauthorized disclosure or retention of classified information, and training in counterintelligence operations. *Id.* He is also familiar through his training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information. *Id.*

Aspects of the offenses that were the subject of the investigation leading to the electronic accounts searches dovetail with this training and experience and with the probable cause to search the defendant's Google account, including the fact that the investigation involved the publication of stolen classified information on the internet; likely involved the transmission of stolen classified information to WikiLeaks using internet-based platforms; and involved communications about the Leaks by the defendant using his Google account. *Supra* 8, 17-18 & Ex. C. "[T]he training and experience of law enforcement agents bear significantly on probable cause determinations. Inferences drawn by law enforcement agents based on facts known to them, the totality of the circumstances, and their training and experience may all support a probable cause finding." *United States v. Mouzon*, No. 16 Cr. 284 (CM), 2016 WL 7188150, at *2 (S.D.N.Y. Dec. 2, 2016) (citing *Illinois v. Gates*, 462 U.S. 213, 231-32 (1983); *see also United States v. Lights*, 208 F. Supp. 3d

568, 575 (S.D.N.Y. 2016) ("A law enforcement agent's expert opinion is an important factor to be considered by the judge reviewing a warrant application.") (cleaned up). The defendant's *ad hominem* and speculative attacks on the affiant's training and experience, Mot. 9-10, in no way contradict or undermine the Affidavit.

The Affidavit similarly establishes probable cause to believe that evidence of the Subject Offenses would be found in the defendant's GitHub account and in the Reddit account. First, the Reddit user identified the defendant as a potential culprit on the same day that the Leak occurred and revealed the connection between the defendant and his username, suggesting some level of knowledge about the defendant and about the Leaks. Ex. C ¶ 28.[3] Second, the Reddit user pointed to a website reflecting the contents of the defendant's GitHub account, which contained (a) computer code, and (b) references to computer applications referenced in the Leak information, suggesting a connection between the contents of the GitHub page and the Leaks. *Id.* ¶ 29. These facts, as well as those discussed above, readily demonstrate probable cause to believe that evidence relating to the Subject Offenses would be found in the Reddit and GitHub accounts. The defendant's proffered innocent explanation—that the referenced computer programs are publicly (by which he means, commercially) available, Mot. 6, does not dispel probable cause, given that the commercially available programs are the very ones referenced in the Leak.

The defendant also argues that the Affidavit presents stale evidence, because the investigation indicated that the classified information in the March 2017 Leak was likely stolen in early 2016. Mot. 10-12. The Court rejected the same argument with respect to the defendant's motion to suppress evidence from his apartment, *see* Supp. Dec. at 12-13, and the defendant's new arguments fail for the same reasons. "The nature of espionage provides that conduct may be

[3] The Affidavit did not assert that the Reddit account was the defendant's.

ongoing because gathering or stealing classified information could have occurred long before the actual transmission," *id.* at 12; and "the affidavit provided facts suggesting ongoing publishing of classified CIA information by Wikileaks—*i.e.*, the March 7 Leak constituted the 'first full part' of a series. Thus, the FBI reasonably could have inferred that Schulte had transmitted classified information from his New York City apartment shortly before the initial Wikileaks publication and could have reasonably inferred that transmission was ongoing." *Id.* at 13.

The Affidavit also describes conduct and events after the suspected date of the theft, including up to the time of the Leaks. As described above, the defendant wrote a draft resignation letter in October 2016 discussing the possibility of stealing classified information and uploading it to the internet, and discussed the Leaks with former colleagues in March 2017. Moreover, that the information published in March 2017 appeared to have been stolen in early 2016, Ex. C ¶ 14(c), indicated that the offense was a continuing one rather than the result of isolated acts occurring in a discrete, known time period. At the time of the Affidavit, it was unknown what additional stolen information would be published and, accordingly, unknown when it might have been stolen or when it might have been transmitted to WikiLeaks. *See* Supp. Dec. at 13; *Singh*, 390 F.3d at 181 ("when the supporting facts present a picture of continuing conduct or an ongoing activity, the passage of time between the last described act and the presentation of evidence becomes less significant") (cleaned up).

The defendant also argues that the only reasonable inference is that he would have deleted any evidence of the theft and transmission of classified information shortly after having stolen it, Mot. 11-12, but (1) the warrant was not limited solely to finding copies of the Stolen Information, but also encompassed evidence of the unauthorized retention, gathering, removal, and transmission of classified documents and materials; and (2) even if there were reason to believe the defendant

would have attempted to delete evidence of his offenses, such deletion attempts are often unsuccessful and the Affidavit described types of information that the defendant would not be able to delete because they were not under his control. *See, e.g.*, Ex. C ¶¶ 5(b)(i) (Google may maintain copies of emails even after deletion by the user), (iv) (transactional and login information), (vii) (location history data), (viii) (device information), (xi) (search and web browser history); ¶ 6 (information maintained by Reddit); ¶ 8 (information maintained by GitHub).

One of the cases the defendant relies on, *United States v. Paul*, 692 F. Supp. 186 (S.D.N.Y. 1988), *see* Mot. 12, undermines rather than supports his contention. There, the court found insufficient reason to believe that an extortion payment would still be located at the defendant's residence five months later and suppressed certain seized cash, but there was no challenge to the seizure of documents and other evidence relating to the defendant's finances. *Paul*, 695 F. Supp. at 191 & n.5; *see also Singh*, 390 F. 3d at 181-82 ("the passage of time is not controlling and is but one factor to be considered, along with the kind of property sought and the nature of the criminal activity, in resolving the issue of probable cause for a search warrant"). Here, similarly, there was ample reason to believe that evidence of the Subject Offenses would be found in the subject electronic accounts even if the defendant had attempted to delete the Stolen Information itself. The Affidavit amply demonstrates a nexus to the searched accounts, and the probable cause was not stale.

4. The Electronic Accounts Warrants Are Sufficiently Particular

The defendant next argues that the warrants to search electronic accounts are insufficiently particular and authorize general searches of the electronic accounts. Mot. 15-25. The defendant's arguments, however, are directed to the categories of data that the providers were ordered to provide to law enforcement pursuant to 18 U.S.C. § 2703(g) in order to be searched for data

responsive to the warrants, and he ignores the provisions of the warrants describing the evidence authorized to be seized out of that data.

The defendant complains that the warrants authorized the seizure of essentially all data contained in his Google and GitHub accounts, Mot. 15-16.[4] That is not the case. The warrants authorized the *search* of a broad set of data, to be produced by the providers. The warrants prescribed that the data from the providers would be reviewed "in order to locate any evidence, fruits, and instrumentalities of" the Subject Offenses, including particularly described categories of evidence, Ex. C-1 at 3-4, in the same way that warrants authorizing the seizure of electronic devices authorize the search of the entire device and its contents for specified categories of data to be seized. Warrants of this type for the seizure and search of electronically stored information have repeatedly been upheld. *See, e.g.*, *United States v. Ray*, 541 F. Supp. 3d 355, 391 (S.D.N.Y. 2021); *United States v. Saipov*, No. 17 Cr. 722 (VSB), 2019 WL 3024598, at *5-8 (S.D.N.Y. July 11, 2019); *United States v. Okparaeka*, No. 17 Cr. 225 (NSR), 2018 WL 3323822, at *9-12 (S.D.N.Y. July 5, 2018); *United States v. Vilar*, No. 05 Cr. 621 (KMK), 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2017).

The defendant next argues that the Affidavit must separately establish probable cause for each category of data produced by the providers. Mot. 20-25. Identifying the particular electronic device or cloud account to be searched satisfies the Fourth Amendment's particularity requirement, and more is not required. *United States v. Guobadia*, 855 F. App'x 27, 29 (2d Cir. 2021) (summary order) ("[T]he warrant, which specifically lists 'computers and computer equipment (card scanners and embossers, printers)' among the items to be seized can hardly be said to lack particularity.").

---

[4] The defendant also challenges the seizure of data from the Reddit account which, as described above, he lacks standing to contest. The warrant to search the Reddit account is, in any event, sufficiently particular for the reasons set forth above.

In support of his argument, the defendant relies on *Riley v. California*, 573 U.S. 373 (2014), and *United States v. Morton*, 984 F.3d 421, *vacated*, 996 F.3d 754 (5th Cir. 2021). No court in this Circuit has held that *Riley* requires probable cause for separate categories of electronically stored information, and the panel decision in *Morton* has been vacated and rehearing *en banc* granted.

Riley does not support the defendant's argument. *Riley* held that the Fourth Amendment does not permit the search of an arrestee's cellphone incident to arrest and that a warrant is generally required. 573 U.S. at 401. The reasoning behind the holding contradicts, rather than supports, the defendant's request that the Court hold that separate probable cause is required for each type of data stored on an electronic device or cloud account. *Riley* treated a cellphone as a single premises, not as a collection of separate premises: "a cell phone collects in one place many distinct types of information." *Id.* at 403; *see also id.* ("before searching a cell-phone seized incident to an arrest" police must obtain a warrant). *Riley* rejected the proposition that it would be reasonable to conduct a warrantless search incident to arrest of only those portions of the cellphone where there was a reasonable belief that evidence would be found. *Id.* at 399. "[O]fficers would not always be able to discern in advance what information would be found where." *Id.* The Court also rejected the proposition that a cellphone could be treated as multiple, discrete premises based on whether there was a non-digital analogue to certain portions of the phone. *Id.* at 400.

The Fifth Circuit panel decision in *Morton* has been vacated and is not precedent for the defendant's proposition. It also contradicts other circuit precedent. In *United States v. Bishop*, the Seventh Circuit rejected the argument the defendant advances here:

> This warrant does permit the police to look at every file on [the defendant's] phone and decide which files satisfy the description. But [the defendant] is wrong to think that this makes a warrant too general. Criminals don't advertise where they keep evidence. A warrant authorizing a search of a house for drugs permits the police to search everywhere in the house, because "everywhere" is where

> the contraband may be hidden. And a warrant authorizing a search for documents that will prove a crime may authorize a search of every document the suspect has, because any of them might supply evidence.

910 F.3d 335, 336-37 (7th Cir. 2018) (citing *United States v. Ross*, 456 U.S. 798, 820-21 (1982); *Andresen v. Maryland*, 427 U.S. 463 (1976); *Steele v. United States*, 267 U.S. 498, 503 (1925)). Other circuits agree. *See United States v. Loera*, 923 F.3d 907, 917 (10th Cir. 2019) ("Our electronic search precedents demonstrate a shift away from considering what digital location was searched and toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant."); *United States v. Bass*, 785 F.3d 1043, 1049-50 (6th Cir. 2015) ("[T]he officers could not have known where this information was located in the phone or in what format"); *see also Guobadia*, 855 F. App'x 27 (a challenged warrant was sufficiently particular by identifying types of electronic devices to be seized).

Lastly, the defendant argues that the Electronic Accounts Warrants lack particularity under *United States v. Wey*, 256 F. Supp. 3d 355, 393 (S.D.N.Y. 2017), because the warrants "set forth 'expansive categories of often generic items subject to seizure—several of a "catch all" variety—without, crucially, any linkage to the suspected criminal activity.'" *See* Mot. 24. This argument ignores part III of Attachment A, which does exactly what the *Wey* decision required: identify the evidence to be located within the seized data by its relation to the Subject Offenses. (Ex. C-1).

In sum, the defendant's challenges to the probable cause supporting the warrants and to their particularity are without merit.

5. The Good-Faith Exception Would Apply

Even if, *arguendo*, the Electronic Accounts Warrants suffered the defects that the defendant asserts, suppression would be inappropriate because the searching agents were entitled to rely in good faith on the warrants issued by the magistrate. *See Falso*, 544 F.3d at 125

(exclusionary rule does not apply to evidence seized in good faith reliance on an issued warrant). In this case, "the fact that a neutral magistrate has issued [the electronic accounts warrants] is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith.'" *Messerschmidt v. Millender*, 565 U.S. 535, 546 (2012) (quoting *Leon*, 468 U.S. at 922-23).

Under the good-faith exception, evidence collected pursuant to an invalid search warrant will be suppressed only if (i) the issuing judge was knowingly misled; (ii) the issuing judge wholly abandoned his or her judicial role; (iii) the application was so lacking in indicia of probable cause as to render reliance upon it unreasonable; or (iv) the warrant is so facially deficient that reliance upon it is unreasonable. *Falso*, 544 F.3d at 125. As set forth above, the defendant fails to show that the Affidavit was either misleading or unreasonably lacking in indicia of probable cause, and he makes no argument that the Court abandoned the judicial role or that the warrant itself was facially deficient. The defendant's attempt to characterize the detailed Affidavit as "bare bones," *see* Mot. 26-27, relies on the same mischaracterizations and selective reading of the Affidavit that the defendant advances elsewhere in his brief.

The defendant fails to satisfy the standard for reconsideration of the Court's prior denial of his motion to suppress the electronic accounts searches and the Motion otherwise fails on the merits for all of the reasons discussed above, and should be denied.

II. The Defendant's Motion to Sever the MCC Counts Should Be Denied

A. Background

As described above, the underlying Second Superseding Indictment charged the defendant with offenses arising out of his unlawful manipulation of CIA computers, his theft of the Stolen Information, and his transmission of the Stolen Information to WikiLeaks in April and May of 2016; offenses arising out of his obstruction of the investigation of the Leaks; and offenses arising

out of his violations of the Protective Order and his transmission and attempted transmission of classified information while at the MCC.

The Second Superseding Indictment also charges offenses arising out of the defendant's receipt and possession of child pornography and violations of the copyright laws, which were severed from the espionage trial without objection. D.E. 117. The defendant's later motion to sever the counts in the Second Superseding Indictment based on his dissemination and attempted dissemination of national defense information from the MCC, based on an alleged advocate-witness issue, was denied. *See* Severance Decision. The Court also rejected the argument that severance of those counts was required to avoid the potential prejudice of evidence of the defendant's pretrial detention or by the defendant's asserted desire to testify in defense of the counts relating to his theft and transmission of the Stolen Information in 2016. *Id.* at 6.

Between February 2 and March 9, 2020, a jury trial was held on the charges in the underlying Second Superseding Indictment, which included charges relating to the defendant's theft and transmission of classified information from the CIA in 2016, the defendant's attempts to obstruct the investigation of the Leaks, and the defendant's transmission and attempted transmission of classified information from the MCC in 2018. The jury returned verdicts of guilty on counts charging the defendant false statements to law enforcement, in violation of 18 U.S.C. § 1001, and contempt of Court, in violation of 18 U.S.C. § 401(3).

The Third Superseding Indictment charges the defendant with several offenses arising from his theft of classified information from CIA computer systems in April 2016 and his transmission of that stolen information to WikiLeaks: illegally gathering national defense information on or about April 20, 2016, 18 U.S.C. § 793(b) (Count One); illegally transmitting unlawfully possessed national defense information between in or about April and May 2016, 18 U.S.C. § 793(e) (Count

Two); unauthorized access of a computer to obtain classified information between on or about April 18 and 20, 2016, 18 U.S.C. § 1030(a)(1) (Count Five); unauthorized access of a computer to obtain information from a department or agency of the United States on or about April 20, 2016, 18 U.S.C. § 1030(a)(2)(B) (Count Six); causing the transmission of a harmful computer program, information, code, or command (*i.e.*, causing the reversion of the network to a snapshot state) on or about April 20, 2016, 18 U.S.C. § 1030(a)(5)(B) (Count Seven); and causing the transmission of a harmful computer program, information, code, or command (*i.e.*, deleting log files) on or about April 20, 2016, 18 U.S.C. § 1030(a)(5)(B) (Count Eight) (collectively, the "WikiLeaks Counts"). The Third Superseding Indictment also charges the defendant with unlawfully transmitting documents, writings, and notes relating to the national defense in or about September 2018, 18 U.S.C. §§ 793(e) and 2, based on his transmission of classified information to the reporter from the MCC (Count Three), and with attempting to unlawfully transmit documents, writings, and notes relating to the national defense between in or about July and October 2018, 18 U.S.C. §§ 793(e) and 2, based on his attempted transmission of classified information from the MCC (Count Four) (together, the "MCC Counts"). Finally, the Third Superseding Indictment charges obstruction of justice arising from the defendant's attempt to obstruct the investigation of the Leaks between approximately March and June 2017, 18 U.S.C. § 1503 (Count Nine).

In the Motion, the defendant asks the Court to sever the MCC Counts from the trial on the remaining charges in the Third Superseding Indictment. Mot. 29-40.

B. Relevant Law

Joinder under Federal Rule of Criminal Procedure 8(a) is appropriate where the counts "are of the same or similar character, or are based on the same act or transaction, or are connected with or constitute parts of a common scheme or plan." Fed. R. Crim. P. 8(a); *see also United States v. Rivera*, 546 F.3d 245, 253 (2d Cir. 2008). Counts that have a "sufficient logical connection" to

each other can be tried together, *United States v. Ruiz*, 894 F.2d 501, 505 (2d Cir. 1990), as can those "where the same evidence may be used to prove each count," *United States v. Blakney*, 941 F.2d 114, 116 (2d Cir. 1991). This Court has "interpreted Rule 8(a) as providing a liberal standard for joinder of offenses." *United States v. Wilson*, 512 F. App'x 75, 76-77 (2d Cir. 2013).

Rule 14(a) provides that "[i]f the joinder of offenses or defendants in an indictment, an information, or a consolidation for trial appears to prejudice a defendant or the government, the court may order separate trials of counts, sever the defendants' trials, or provide any other relief that justice requires." Fed. R. Crim. P. 14(a). The decision to grant or deny severance under Rule 14 is "committed to the sound discretion of the trial judge." *United States v. Spinelli*, 352 F.3d 48, 54 (2d Cir. 2003). That the counts at issue are "sufficiently logically linked" and would require much of the same evidence weighs against severance. *United States v. Page*, 657 F.3d 126, 129 (2d Cir. 2011). It is not enough to demonstrate that separate trials would increase the chances of the defendant's acquittal, *see United States v. Burke*, 700 F.2d 70, 83 (2d Cir. 1983); rather, the defendant "must show prejudice so severe as to amount to a denial of a constitutionally fair trial." *United States v. Serpoosh*, 919 F.2d 835, 837 (2d Cir. 1990); *see also United States v. Walker*, 142 F.3d 103, 110 (2d Cir. 1998) ("A defendant seeking severance must show that the prejudice to him from joinder is sufficiently severe to outweigh the judicial economy that would be realized by avoiding multiple lengthy trials.").

C. Argument

The Court denied the defendant's prio request to sever counts relating to his dissemination and attempted dissemination of national defense information while incarcerated at the MCC from the other charges in the Second Superseding Indictment, *see* Severance Decision; and those counts in fact were tried along with other counts in the prior trial. Notably, the Motion does not point to a single instance of prejudice in the entire trial record or even refer to the trial record at all. The

defendant offers no basis to reconsider the denial of his prior severance request, and the Motion should be denied.

The offenses charged in the MCC Counts and the offenses charged in the WikiLeaks Counts are of "similar character" and part of a "common scheme or plan," are "logically linked," and proof of both sets of counts involves overlapping evidence. Accordingly, joinder is proper under Rule 8(a). For example, evidence of the defendant's motive and intent for the intentional theft and dissemination of the Stolen Information in 2016, a reaction to perceived grievances against the CIA, is also evidence of the defendant's motive and intent to unlawfully transmit national defense information in 2018 as part of an "Information War" against the United States government by whom the defendant feels aggrieved, *see* D.E. 410 at 17-22, and vice versa. The manner in which the defendant evaded of controls over the DevLAN network and attempted to destroy evidence of his crimes in order to clandestinely exfiltrate the Stolen Information from the CIA in 2016 is evidence relevant to the defendant's motive and intent in using contraband cellphones, unattributed email and social media accounts, and encrypted email facilities to communicate about and disseminate national defense information from the MCC in 2018, *id.* 19-22, and vice versa. The defendant's 2018 plans to fabricate evidence that he was framed for the 2016 theft of the Stolen Information, *e.g.* GX809 at 9-13, is relevant evidence of guilty conscience. The national defense information the defendant unlawfully disseminated and attempted to unlawfully disseminate from the MCC in 2018 includes both classified information contained in the Leaks (which the defendant originally stole) as well as other information the defendant knew from his time at the CIA. The defendant's knowledge relating to national defense information gained from his time at the CIA is relevant to both episodes of his unlawful transmission of national

defense information. The groups of counts are plainly logically linked by evidentiary basis, type of conduct, and related underlying facts.

The defendant argues that the groups of counts are not similar because "there is no factual overlap" between the two groups and distinct evidence relating to both groups,[5] Mot. 30; are not based on the same act or transaction and not part of a common scheme or plan, *id.* at 31; the defendant's purported defenses are "substantially different" as to each group of counts, *id.* at 32; and "the MCC counts are fundamentally different from the WikiLeaks counts in terms of the context in which the disclosures allegedly took place, the subject matter of the information allegedly disclosed, and the parties to whom that information was allegedly disclosed," *id.* The defendant's arguments mischaracterize the nature of the charges and the evidence supporting them, *supra*; and further misunderstand the meaning of "similar character." "Similar" means "early corresponding; resembling in many respects; somewhat alike; having a general likeness." *United States v. Werner*, 620 F.2d 922, 926 (2d Cir. 1980) (Friendly, J.) (upholding joinder of counts arising from distinct episodes involving similar crimes). The WikiLeaks Counts and MCC Counts are easily "similar" under this definition.

The defendant next argues that severance should be granted because trial on the MCC Counts can be held faster than a trial on the WikiLeaks Counts. Mot. 33. Trial on both sets of counts is currently scheduled for June 13, 2022 and severance would delay, rather than speed, the resolution of the charges.

Finally, the defendant argues that joinder prejudices him because evidence of the MCC Counts will alert the jury that he has been incarcerated pending trial, *id.* 34, 35-36; the jury may

[5] The defendant argues that the evidence on the WikiLeaks Counts is "almost non-existent," Mot. 30, despite the fact that those counts are supported by voluminous electronic and documentary evidence and witness testimony.

be confused about the defendant's defenses to each group of counts, *id.* 34, 36-39; and the defendant intends to testify in his own defense with respect to the WikiLeaks Counts but not the MCC Counts because of the risk of cross-examination about his conduct at the MCC. *Id.* 34, 39-40. None of these arguments has any merit. As the Court previously held, neither the "prejudice of pretrial detention" nor "juror confusion . . . mandate the severance Schulte seeks." Sev. Dec. at 6. The risk of prejudice resulting from evidence of the defendant's pretrial detention can be addressed at trial, including through jury instructions, *see* D.E. 256 at 3 ("The probative value of the evidence [showing the defendant's incarcerated status] is not substantially outweighed by prejudice under FRE 403. The Court will issue a limiting instruction."); and the defendant will have an opportunity to address the jury in opening and closing statements to clarify any distinctions between his defenses to the two sets of counts.[6]

Nor do the defendant's representations regarding his intention to testify justify severance. "[N]o need for a severance exists until the defendant makes a convincing showing that he has both important testimony to give concerning one count and the strong need to refrain from testifying on the other." *United States v. Sampson*, 385 F.3d 183, 191 (2d Cir. 2010). "In making such a showing, it is essential that the defendant present enough information—regarding the nature of the testimony he wishes to give on one count and his reasons for not wishing to testify on the other—to satisfy the court that the claim of prejudice is genuine" and to allow the court to weigh that prejudice against the efficiencies of joinder. *Id.* Here, the defendant's proffer of his supposedly conflicting desires to testify on some counts and not on others provides little information about the

[6] Moreover, the defendant's proffered defenses are not inconsistent with each other: the defendant claims someone else committed the theft of the Stolen Information, and that it was not illegal for him to disseminate national defense information in 2018 to the extent that information was publicly available on the internet. The defendant suffers no substantial prejudice from seeking to advance both defenses at trial.

nature of the testimony he would offer and shows no genuine prejudice. The defendant says only that he would "testify about the facts and circumstances surrounding his employment at the CIA, including the nature of his job, the various projects he worked on, and the reasons for his conduct with respect to specific CIA technical projects and systems" and "as to why the government incorrectly identified him as one of the few possible individuals who could have extracted classified information from CIA backup systems during the time period in question." Mot. 39-40. This generic description is unilluminating as to what testimony the defendant intends to offer or why he wants to offer it, and fails to satisfy his burden under *Sampson*.

Moreover, the defendant's proffered reasons for not wanting to testify with respect to the MCC Counts, Mot. 40, do not demonstrate genuine prejudice. Evidence of his conduct at the MCC would be admissible, *supra* 30-31, and he would be subject to cross-examination about it, even if the MCC Counts were severed from the WikiLeaks Counts. That conduct is relevant to the defendant's motive, knowledge and intent in committing the offenses charged in the WikiLeaks Counts and to his identity as the person who committed the offenses, *see* Fed. R. Evid. 404(b); it involves specific instances of the defendant's conduct relevant to his truthfulness, *see* Fed. R. Evid. 608(b); and his conduct at the MCC includes his prior statements concerning the WikiLeaks Counts, *see* Fed. R. Evid. 613. Evidence of the defendant's conduct in connection with the WikiLeaks Counts, similarly, would be admissible at a severed trial on the MCC Counts.

The defendant fails to satisfy the standard for reconsideration of the Court's prior denial of his motion to sever the MCC Counts and the Motion otherwise fails on the merits for all of the reasons discussed above, and should be denied.

III. The Court Has Already Rejected the Basis for the Defendant's Motion to Preclude, Which Is Without Merit

The defendant's motion to preclude the Government from using evidence obtained from digital forensic analysis of CIA computer systems is based entirely on the proposition that he has been denied discovery to which he claims to be entitled. But as the defendant acknowledges, the Court has previously ruled twice that he is not entitled to the material that he demands. *See* Mot. 40. As was true with the defendant's previous demands, the instant motion "articulates no specific rationale for why he should be entitled to mirror images of two entire servers containing troves of classified material with no relevance to this action whatsoever." NetApp Discovery Dec. at 4. The Court should not "authorize the wholesale sifting of haystacks of irrelevant, sensitive national security information based on the speculative, theoretical hope of discovering an as-yet-undisclosed needle of relevance." *Id.* at 5.

The defendant cannot meet the demanding standard for reconsideration of the Court's prior rulings that he is not entitled to full mirror images containing vast sensitive national security information irrelevant to this case. Because he has not been denied any information to which he is entitled, no preclusion is appropriate.

Even taken on their merits, however, the defendant's claims premised on the Due Process and Confrontation Clauses are groundless. Although the defendant has not been provided with full mirror images, he has been provided with all the facts and data that underlie the actual conclusions to which the Government's expert testified and will testify, and his generic assertions to the contrary do not establish that he has been denied any relevant material.

A. Applicable Law

The Government's discovery obligations in criminal cases begin with Federal Rule of Criminal Procedure 16(a)(1), which provides, in pertinent part, that the Government must disclose

to the defense documents and objects that are "within the government's possession, custody, or control" if they are "material to preparing the defense" or will be used by the Government in its case-in-chief at trial. Evidence is material to the defense "if it could be used to counter the government's case or to bolster a defense," but "information not meeting either of those criteria is not to be deemed material within the meaning of" Rule 16. *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993) (interpreting the Rule's predecessor, Fed. R. Crim. P. 16(a)(1)(C)). "Materiality means more than that the evidence in question bears some abstract logical relationship to the issues in the case. There must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *United States v. Maniktala*, 934 F.2d 25, 28 (2d Cir. 1991) (internal quotation marks omitted). In addition, with respect to the Government's obligations to disclose materials related to its experts, Federal Rule of Criminal Procedure 16(a)(1)(G) requires that the Government must disclose a "written summary of any testimony that the Government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial" and that the summary describe "the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications." Federal Rule of Evidence 705 permits an expert to "state an opinion—and give the reasons for it—without first testifying to the underlying facts or data" but also states that "the expert may be required to disclose those facts or data on cross examination."

Of course, the Government also has an obligation under the Due Process Clause to disclose to the defendant exculpatory and impeaching evidence. *See Brady v. Maryland*, 373 U.S. 83 (1963); *Giglio v. United States*, 405 U.S. 150 (1972). But "[t]here is no general constitutional right to discovery in a criminal case, and *Brady* did not create one." *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977); *see also United States v. Polowichak*, 783 F.2d 410, 414 (4th Cir. 1986) ("*Brady*

did not create a criminal right analogous to discovery in a civil case."); *United States v. Evanchik*, 413 F.2d 950, 953 (2d Cir. 1969) ("Neither [*Brady*] nor any other case requires the government to afford a criminal defendant a general right of discovery."). Nor does the defendant have a "constitutional right to conduct his own search of the [Government's] files to argue relevance." *Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987). "Unlike Rule 16 and the Jencks Act . . . *Brady* is not a discovery rule, but a rule of fairness and minimum prosecutorial obligation . . . ." *Maniktala*, 934 F.2d at 28 (internal quotation marks omitted). It is the prosecution team's duty to evaluate whether exculpatory information existed within its holdings. *See United States v. Agurs*, 427 U.S. 97, 109 (1976) ("If everything that might influence a jury must be disclosed, the only way a prosecutor could discharge his constitutional duty would be to allow complete discovery of his files as a matter of routine practice. . . . [T]he Constitution surely does not demand that much.").

Nor is the defendant's interest the only factor to be assessed in determining whether he is entitled to sensitive national security information. "When determining whether discoverable, helpful, and material classified material should be disclosed to the defense, 'the test to be applied involves balancing the defendant's need for the information or its value to the defendant, against the possible damage to the government's security interests from disclosure.'" Section 4 Dec. at 5 (quoting *United States v. Rahman*, 870 F. Supp. 47, 52 (S.D.N.Y. 1994)). "[C]lassified information is not discoverable on a mere showing of theoretical relevance in the face of the Government's classified information privilege." *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989).

B. Argument

The defendant first articulated his claims that the denial of access to mirror images of CIA computer systems amounted to a violation of due process and prevented effective cross-examination in a motion for mistrial during the first trial in this case, *see* D.E. 328 at 3, 8-12; and renewed those arguments in a letter dated July 28, 2020, *see* D.E. 420. As in the instant motion,

the defendant has argued that the fact that the Government's expert had access to the complete images necessarily entitles the defendant to them as well, on the ground that the Constitution precludes the Government "from relying on evidence and information that it refuses to provide to the defense for reciprocal discovery and cross-examination." Mot. 46.

As the Government explained in response, however, *see generally* D.E. 423, the actual record belies the defendant's distorted claims. The Government has complied with its disclosure obligations by providing the defendant with all of the facts and data upon which the Government's expert, Patrick Leedom, based his opinions. Mr. Leedom's lengthy testimony—spanning nearly 300 transcript pages, Tr. 908-1201—and voluminous expert report, GX1703, make clear that none of the opinions to which Mr. Leedom testified or will testify relied on any information from the complete images beyond what was produced to the defense. Rather, Mr. Leedom testified specifically about particular forensic artifacts taken from those servers and explained how those artifacts supported his opinions.

Well in advance of trial, the Government produced extensive forensic discovery to the defendant to enable him and his expert to conduct their own analysis. *See* D.E. 329 at 8-10 (describing forensic discovery). Starting in July 2019, the Government began to identify the specific forensic artifacts underlying Mr. Leedom's opinions. Moreover, the Government produced a detailed expert notice to the defense on October 18, 2019 (specificially stating that Mr. Leedom's opinions were based on the forensic materials produced in discovery to the defendant), and began producing drafts of Mr. Leedom's trial presentation weeks before trial. The Government also produced extensive both classified and unclassified materials pursuant to 18 U.S.C. § 3500 in which Mr. Leedom documented his analytic process. The defendant now of course has the benefit of Mr. Leedom's entire trial testimony. He still is unable to articulate any reason why the forensic

discovery produced to him is insufficient beyond a generic claim that anything less than complete access will not do, and he does not identify a single aspect of Mr. Leedom's substantive testimony that he has insufficient information to challenge.[7]

Schulte's assertion that "[t]here is no way to know what data is relevant and critical until a full examination is performed," Mot. 45, is both incorrect and contrary to applicable law. It is beyond cavil that he has no "constitutional right to conduct his own search of the [Government's] files to argue relevance," *Ritchie*, 480 U.S. at 59, and that "[t]he mere possibility that an item of undisclosed information might have helped the defense . . . does not establish 'materiality' in the constitutional sense," *Agurs*, 427 U.S. at 109. Rather, "[t]he defendant must make a prima facie showing of materiality and must offer more than the conclusory allegation that the requested evidence is material." *United States v. Weigand*, No. 20 Cr. 188 (JSR), 2020 WL 5105481, at *11 (S.D.N.Y. Aug. 31, 2020) (internal quotation marks omitted). This is particularly true under the Classified Information Procedures Act ("CIPA"), Title 18, U.S.C., App. III, where "'classified information is not discoverable on a mere showing of theoretical relevance.'" *United States v. Abu-Jihaad*, 630 F.3d 102, 142 n.35 (2d Cir. 2010) (quoting *Yunis*, 867 F.2d at 622)). As Judge Crotty noted, allowing the defendant the unfettered access that he seeks "would be to undermine the fundamental purpose of CIPA." *See* NetApp Discovery Dec. at 5.

For these reasons, the cases that Schulte relies on are neither persuasive nor on point. As was true in his earlier motions on this subject, "[t]he cases Schulte relies upon in support of his equal access theory are not CIPA cases." *Id.* at 4. For example, the defendant quotes from *United*

[7] In his original motion for a mistrial, the defendant's former counsel did attempt to identify particular "examples of prejudice" arising from their lack of access to the mirror images. (*See* D.E. 328 at 9-12). The Government provided detailed responses to each claim, noting the discovery that had been produced responsive to each one. (*See* D.E. 329 at 17-20).

States v. Zanfordino, 833 F. Supp. 429, 432 (S.D.N.Y. 1993) in support of his claim that the failure to provide him with the full images impaired his rights under the Confrontation Clause. *See* Mot. 44. But that case specifically noted that there was no claim of "governmental privilege . . . which would militate against the disclosure of material prepared or utilized in connection with analysis of the footprints and sneakers involved in this case," and cited the informant's privilege set forth in *Roviaro v. United States*, 353 U.S. 53 (1957)—which applies in CIPA cases, *see United States v. Aref*, 533 F.3d 72, 79-80 (2d Cir. 2008)—as an example of such a privilege. *Zanfordino*, 833 F. Supp. at 433. Moreover, the disclosures provided to the defendant here comply with the concerns expressed in that case. The fact that Mr. Leedom had access to the full images does not mean that he "is testifying based in part on undisclosed sources of information," *id.* at 432, because the specific sources of information underlying his testimony have not only been disclosed, but identified with particularity for the defendant.

The Government is mindful of the Court's admonition of the Government's relevant disclosure obligations. *See* NetApp Discovery Dec. at 5-6. Throughout this case, the Government has undertaken extensive steps to ensure the defendant's ability to prepare and present his defense while still protecting irrelevant but highly sensitive national security information. That has included not only the Government's careful evaluation of what information might conceivably be relevant and helpful to the defendant, Section 4 Dec. at 11, but also continued responses to defense requests that "articulated a justifiable need for additional material," *id.* at 10; *see also* D.E. 329 at 9-10 (describing additional productions in response to defense requests). The defendant has not been denied any relevant or helpful material to which he is entitled, nor has the Government offered (nor does it intend to offer) any expert testimony based on any forensic materials that have

not been produced to the defendant. Accordingly, there is no basis to deviate from the Court's prior rulings, and the Motion to preclude should be denied.

IV. The Motion to Compel Is Largely Moot and Should Otherwise Be Denied

The defendant seeks to compel classified productions of "the CIA's Stash and Confluence backups that were allegedly stolen and transmitted to WikiLeaks, all emails and sametime [chat] messages sent and received by Mr. Schulte, and Mr. Schulte's complete CIA polygraph results." Mot. 47. All of these demands have previously been addressed either by the Government's discovery productions or by prior rulings of the Court.

A. Stash and Confluence Backups

The Government has alleged that the information disseminated by WikiLeaks was derived from daily backup files for the Confluence and Stash[8] servers created on March 3, 2016. On December 10, 2018, the Government produced the March 3 and 4, 2016 Confluence backups (*i.e.*, the backup that was stolen and the one immediately after it) on December 10, 2018. On November 5, 2019, in response to a defense request specifically made in connection with the Government's October 18, 2019 expert disclosures regarding the timing analysis of the leaked material conducted by Michael Berger,[9] the Government and the CIA arranged for a standalone laptop (the "Standalone") to be made available in CIA space for review by defense counsel and the defense

[8] Confluence is a Wikipedia-like platform used by EDG where users could post comments about the group's work. Stash is a repository for, among other things, source code that was used by EDG. (Trial Tr. 174, 215-18).

[9] At trial, Mr. Berger testified (as had previously been explained in two detailed expert reports provided in October 2018 with the Government's expert notice) that his timing analysis was based on version control of the daily backups of Stash and Confluence, that is, he "looked for examples of data points of data that was saved in the system that was present on WikiLeaks. And data that was saved in the system that was not present on Wikileaks. . . . So looking at the data that was both present in the database and present on WikiLeaks, and present in the database and not present on the WikiLeaks, we were able to determine at what point the data sort of stopped that WikiLeaks has." (Tr. 1352, 1357).

expert. The Standalone was loaded with (1) complete, unredacted copies of the March 2 and 3, 2016 Confluence databases and all of the Confluence data points used by Mr. Berger to conduct his timing analysis; (2) complete, unredacted copies of the Stash repositories for the tools for which source code had been released by WikiLeaks; (3) complete, unredacted copies of all Stash documentation released by WikiLeaks; and (4) all commit logs (*i.e.*, the record of changes made to particular projects) for all projects released by WikiLeaks, redacting only names of the particular users that made those changes. The defendant's expert examined the Standalone in December 2019.[10] *See* D.E. 332 (describing information provided to the defendant's expert).

Thus there is no question that the defendant has already been provided with the allegedly stolen backups, with the Confluence backups for the days preceding and following the theft, the entire Stash repositories for the materials released by WikiLeaks, and with all of the specific data points of information on which Mr. Berger based his testimony, along with detailed reports identifying the specific files Mr. Berger examined and the analysis that led to his conclusions. Every exhibit introduced at trial, and every item necessary to "reproduce Berger's timing analysis" Mot. 50, or to conclude that it was incorrect, has been produced to the defense. For example, the defendant and his expert are freely able to evaluate whether there are changes reflected in the March 3, 2016 Confluence backup that are not reflected in the material disclosed by WikiLeaks, or likewise whether there is information on WikiLeaks not contained in that backup that would suggest Mr. Berger's analysis is wrong. Mr. Berger's analysis was precise as to the specific backup file reflected in the disclosed material; the defense also has access to the two surrounding

[10] The defense did not raise any issues with the materials provided on the Standalone or make any more tailored requests, but simply insisted to the Court, before the expert had even examined the Standalone that as a blanket matter, the Government's production was insufficient. *See* Nov. 13, 2019 Tr. at 5-8.

backups—March 2 and 4, 2016—which would enable him similarly to identify if there is material there that either is, or is not, included in what was disclosed. Similarly, the defendant's expert has the ability to compare the Stash data released by WikiLeaks with the entire commit logs for those projects to determine what are the last changes to that data reflected in the released versions—the same analysis Mr. Berger performed.[11] But other than generically averring that the Government's production was insufficient, the defendant identifies no aspect of Mr. Berger's analysis that he is unable to challenge.

Nevertheless, the defendant demands access to "all the Stash and Confluence backup files in the CIA's possession." Mot. 49. But as with his demand for complete mirror images, the defendant is asserting a non-existent "constitutional right to conduct his own search of the [Government's] files to argue relevance." *Ritchie*, 480 U.S. at 59. To analogize to another form of forensic analysis, the defendant's claim is akin to asserting that because the Government intends to offer testimony that DNA found at a crime scene matched the defendant's DNA, the defendant is entitled to discovery of the Government's DNA databases so that his expert can search for a better match. But the Constitution does not require such trolling. *Cf. United States v. Johnson*, No. 11 Cr. 1, 2011 WL 4729966, at *1, 3-4 (N.D. Ohio Oct. 7, 2011) (denying defense request for "information regarding other potential matches identified by [the Government's expert's] comparison of the partial DNA profile collected from the hat with the CODIS database," noting that the "mere possibility that the information sought might help the defense does not establish that this evidence is material"). To be clear, the Government is unaware of any other information

[11] On January 28, 2020, the Government also produced, in response to the defense's request, additional metadata for the backups showing that the March 3, 2016 Confluence backup files were accessed during the defendant's manipulation of the CIA computer systems on April 20, 2016, and that the March 3, 2016 Confluence backups were the only backup files that had ever been accessed on a date other than that on which they were created.

contained in the backups that have not been produced that would contradict or otherwise cast doubt on Mr. Berger's conclusions or any other aspect of the Government's case, and is mindful of its obligation to produce any such information of which the Government learns. The primary information the defendant seeks has been produced to him, and he articulates no insufficiency that would support his broader demand.

B. Email and Chat Messages

The defendant next argues that the Government must produce "all emails and Sametime messages both sent and received by Mr. Schulte." Mot. 51. The Court has already denied this request and granted the Government's motion pursuant to CIPA § 4 to withhold any additional materials from the defendant's email and chat records. *See* Section 4 Dec. at 9. As the Court has already noted, "[t]he Government conducted a review of every email and chat sent by or to Schulte, but produced only those documents it viewed as relevant to the charged conduct, with redactions to certain classified information," but was also "willing to supplement its production by producing all of Schulte's sent email communications during the relevant time period." *Id.* Thus, in addition to the email and chat messages that the Government identified as relevant, the Government has also produced all of the defendant's sent emails from the CIA at any point from 2015 to 2016. The Court has already concluded that this "compromise comports with [the Government's] obligations under Rule 16 and CIPA." *Id.*

That conclusion was correct, and Schulte offers no reason to revisit it. By its terms, Rule 16(a)(1)(B) applies only to a "*relevant* written or recorded statement by the defendant" (emphasis added). It is well-established that "Rule 16 thus does not cover . . . statements unrelated to the crime charged or completely separate from the Government's trial evidence." *United States v. McElroy*, 697 F.2d 459, 464 (2d Cir. 1982); *see also United States v. Scarpa*, 897 F.2d 63, 70 (2d Cir. 1990) (affirming refusal to order disclosure of recorded conversations of the defendant that

were "either wholly innocuous or involve[d] criminality that has nothing to do with the crimes charged in this case"). The Government has exceeded this obligation by producing every email sent by the defendant for a two-year time period, along with hundreds of other emails that he received (as well as hundreds of emails sent or received by other employees with whom the defendant worked that were produced as § 3500 material). Nothing further is required.

C. Polygraphs

Finally, the defendant asserts that he has been denied information from his 2016 CIA polygraph that would "demonstrate that the CIA exonerated him of any wrongdoing through its own internal testing." Mot. 52. As background, the defendant was required to participate in a polygraph investigation in September 2016 as part of routine security clearance reinvestigation processing. The defendant resigned from the CIA in November 2016, however, and so, as the Government has repeatedly informed the defendant, that polygraph was never "adjudicated," and no determinations either as to the defendant's polygraph itself or the broader security clearance reinvestigation were ever made. *See* Section 6(a) Dec. at 6 (noting that the Government had informed the Court that "there are no results for the polygraph because Schulte left the CIA before it was adjudicated"). The Government nevertheless produced the transcript of the polygraph to the defendant in classified discovery.

The defendant previously moved for additional discovery related to the polygraph and to introduce evidence related to it at trial. The Court ruled that the defendant "can testify as to having taken the 2016 polygraph to demonstrate consciousness of innocence," but that because "there are no results for the polygraph[,] . . . the Court is not concerned about the general reliability of polygraph results or objections under Rule 702. To the extent the Defendant seeks to admit the [transcript of the polygraph] for its statements the document is inadmissible hearsay." *Id.* at 5-6.

There is nothing whatsoever to suggest that "the CIA exonerated" the defendant in his polygraph, Mot. 52—no determination was ever made. While it is doubtful that in any case the defendant would be entitled to "the CIA's vast trove of polygraph and scientific data," *id.*, here there is no basis for disclosure of the reliability of CIA polygraph procedures more generally because the defendant's 2016 polygraph was never adjudicated. Separate from the specifics of the defendant's case, "[b]oth the United States Supreme Court and [the Second Circuit] have repeatedly upheld the exclusion of polygraph evidence because of its unreliability, its potential to confuse the issues and mislead the jury, and the danger of unfair prejudice posed by its admission." *United States v. Fraser*, 206 F. App'x 100, 101 (2d Cir. 2006) (citing *United States v. Scheffer*, 523 U.S. 303, 309 (1998); *United States v. Kwong*, 69 F.3d 663, 668 (2d Cir. 1995); *United States v. Rea*, 958 F.2d 1206, 1224 (2d Cir. 1992)). Neither technological advancement nor what the defendant claims are the different methodologies employed by the CIA change the fundamental flaw that has always precluded the admission of polygraph evidence: "Polygraph tests are unreliable in that the examiner must extrapolate a judgment of something not directly measured by the machine, *i.e.*, the credibility of the person examined." *United States v. McCants*, No. 86 CR. 163 (JMW), 1986 WL 7273, at *1 (S.D.N.Y. June 26, 1986).

Put simply, the "ultimate determination" of the defendant's polygraph that he seeks, Mot. 52, does not exist. Accordingly, the rest of his requests are academic, because however reliable the CIA's polygraph determinations may be when they are made, no determination was made in his case.

V. The Defendant's Motion to Suppress Documents Seized Pursuant to the MCC Search Warrants Should Be Denied

A. Background

1. The MCC Search Warrants

On October 2, 2018, the Government applied for a warrant (the "MCC Premises Warrant") to search two units at the MCC (including the one in which Schulte was housed) and the MCC's law library (the "MCC Premises"). *See* Ex. E-1. The affiant, Special Agent Donaldson, first described the circumstances of Schulte's detention at the MCC (including his theft of the Stolen Information), Ex. E ¶¶ 8(a)-(t), and that Schulte was housed in the same unit as another inmate, Omar Amanat, who had been convicted of fraud offenses and who had fabricated evidence at trial, *id.* ¶¶ 9 & 12. Agent Donaldson went on to state that, in or about April 2018, Schulte sent at least one of the 2017 warrants to a reporter in violation of the Court's protective order, resulting in the Court's reprimand on May 21, 2018. *Id.* ¶¶ 11(a)-(d). Finally, Agent Donaldson described information that the FBI had received from another inmate (the "CS"), who had informed the FBI that, among other things, Schulte and Amanat were using Contraband Cellphones in the MCC, and that the CS recalled at least one conversation over one of the Contraband Cellphones in which "Vault 7," the name for the 2017 WikiLeaks disclosures, had been discussed. *Id.* ¶ 13. The CS also provided the FBI with screenshots and videos of Schulte and Amanat using the Contraband Cellphones to, among other things, disseminate documents they had drafted. *Id.* ¶ 15. Based on this application, the Court authorized the search of the MCC Premises, including for the Contraband Cellphones and any documents and records pertaining to the illegal gathering, retention, removal, and transmission of classified information, including in particular nine "articles" Schulte had drafted (the "Schulte Articles"). *Id.* ¶ 6.

On October 3, 2018, the FBI began to search the MCC Premises. During the search, MCC officials gave the FBI documents from the cell Schulte had inhabited before his October 1, 2018 transfer to a secure housing unit (the "Schulte Cell Documents"), including loose files and several notebooks and notepads (the "Notebooks"). *See* Ex. F ¶ 6(a). The cover of each of the Notebooks was labeled with the words "ATTORNEY-CLIENT PRIVILEGE." FBI agents flipped briefly through the Schulte Cell Documents and confirmed that they appeared to contain handwritten text potentially written by Schulte. The agents opened to a small subset of pages in each Notebook at random, and made a cursory examination of the legible text on those pages. During that review, the agents identified some writings that appeared to be potentially classified. The agents, however, were not sure whether these documents fell within the ambit of the MCC Premises Warrant. Among some of the loose files, the agents also saw, among other things, cover pages marked with Trulincs, which the agents understood might relate to Schulte's defense. D.E. 120 at 60.

Based on these findings, the agents immediately informed the prosecutors about the discovery of the Schulte Cell Documents. The prosecutors told the agents to stop reviewing the Schulte Cell Documents until further instruction. *Id.* at 60-61. The Government then sought an addition warrant ("the MCC Wall Warrant") for authorization to search the Schulte Cell Documents for evidence of the same crimes as those identified in the MCC Premises Warrant. *See* Ex. F-1. Because the agents had noticed potentially privileged documents, the Government sought authorization for a wall review process to search the Schulte Cell Documents. *Id.*

The affidavit for the MCC Wall Warrant described that "before the search began, MCC officials had removed the Schulte Cell Documents, among other things, from Schulte's former cell and stored them in an official office at the MCC." Ex. F ¶ 6(a). The Schulte Cell Documents were "comprised of approximately 300 pages of material," which the FBI agents "began to review"

during the search of the MCC Premises. *Id.* ¶¶ 6(b). During that initial review, Agent Donaldson described how the agents had found, among other things, copies of the Schulte Articles, an email account that was accessed from one of the Contraband Cellphones and the password to that account (the "John Smith Document"), and a document purportedly authored by an FBI agent (the "FBI Document") and intended for WikiLeaks, in which the author claimed that Schulte was not responsible for the Leaks and that the FBI had planted child pornography on Schulte's computer. *Id.* The agents also saw, however, some markings on the documents that indicated that some of the documents "were potentially prepared to aid in Schulte's defense." *Id.* ¶ 6(c). A wall review team (the "Wall Team") would review the Schulte Cell Documents for any privileged material and then tum over any non-privileged material to the FBI case agents to review. *Id.* ¶ 7. That review was to be completed within 48 hours. *Id.* ¶ 8. The Court granted the Government's application.

Within the prescribed time, the Wall Team reviewed the Schulte Cell Documents, redacted material that the Wall Team had determined to be privileged, and provided the redacted versions to the case team. The Wall Team also provided both redacted and unredacted copies of the Schulte Cell Documents to the defense. The Government also provided the redacted versions of the Schulte Cell Documents to the CIA for a classification review. In reviewing the redacted versions of the Schulte Cell Documents, the case team noted that, in addition to the John Smith Document and the FBI Document, the Schulte Cell Documents also included among other things, (i) information about social media (the "Social Media Accounts") and the Encrypted Accounts that Schulte had or intended to create, including passwords for those accounts; (ii) a draft tweet that contained classified information and in which Schulte purported to be one of his former CIA colleagues, who claimed that the CIA had framed Schulte (the "Fake Tweet"); (iii) threats by Schulte to begin an "information war" against the United States, during which he would disclose additional classified

information, unless he was released and paid restitution, (iv) Schulte's list of steps to destroy evidence, including deleting "suspicious emails" from accounts he was using in prison; (v) Schulte's notations to "DL Disc. UL WL," which the FBI understood to likely mean downloading Schulte's discovery ("DL Disc.") and uploading it to WikiLeaks ("UL WL'') and to "schedule tweets;" (vi) notes about apparent segments of memory in a laptop where data could be hidden; (vii) a note to "check Galaxy [the model of one of the Contraband Cellphones] for Signal" (an encrypted messaging application); and (ix) a loose "article" titled "Malware of the Mind" (the "Malware Article") addressed to the technology community, which contained classified information about Schulte's CIA training.

Based in part on these findings, the Government applied for additional search warrants including the Encrypted Email Warrant; the Social Media Warrant; and the Laptop Warrant. The Court granted the Government's application for each of these Warrants. The searches conducted pursuant to these Warrants also uncovered significant evidence against Schulte, including an email that he sent to a reporter in September 2018, in which Schulte claimed to be a third party speaking on Schulte's behalf and attached a document that purportedly rebutted the probable cause in one of the 2017 Warrants and contained classified information.

2. The Defendant's Prior Motions to Suppress and to Exclude

On June 18, 2019, the defendant filed a motion to suppress evidence seized pursuant to the MCC Warrants, *see* D.E. 98, arguing that the initial search pursuant to the MCC Premises Warrant exceeded the scope of the warrant by "indiscriminately seiz[ing]" all of the defendant's notebooks from his cell, *id.* 8-10; that the executing agents acted in bad faith by intentionally invading the defendant's attorney-client privilege, *id.* 10-14; that the Wall Team did not protect the defendant's privilege, *id.* 14-18; and that the subsequent MCC Warrants were the fruit of the poisonous tree.

Id. 18-19. In the alternative, the defendant moved to suppress pages from the Notebooks that were unredacted by the Wall Team. *Id.* 20-21.

The Court denied the motion by Opinion and Order dated October 18, 2019. MCC Suppression Decision. The Court found that the defendant's self-labeling of the Notebooks as "attorney-client privilege" did not render them privileged and did not require the executing agents to assume that they were, and that it was not unreasonable for the agents to conduct a cursory review of the contents Notebooks to determine relevance and then consult the prosecution team. *Id.* at 5-6. The Court further held that the wall review procedure was reasonable, *id.* at 6-7; and that the motion to suppress had failed to carry the defendant's burden of showing that any of the documents seized were, in fact, privileged. *Id.* at 7-8. The Court held that, if the Government sought to introduce privileged documents at trial, the defendant could move to suppress allegedly privileged documents at that time. *Id.* at 8.

On November 27, 2019, the Government moved *in limine* to introduce, among other things, portions of the Notebooks from which privileged information had been redacted, D.E. 195 at 34-35; and the defendant opposed, arguing, *inter alia*, that the Notebooks and the Malware Article were privileged or work product. *See* D.E. 242 at 23-24. The Court directed that the Government identify the specific documents sought to be introduced, D.E. 252 & 256 at 3; and the Government identified particular selections of two of the Notebooks and of the Malware Article. *See* D.E. 257. The defendant responded, identifying specific portions of the selections identified by the Government as privileged or work product, but otherwise arguing only that the documents should be excluded on the basis of relevance and prejudice. *See* D.E. 282. In response, the Government agreed to redact those portions of the selected documents over which the defendant asserted privilege or work product. *See* D.E. 285. The Court ruled that the exhibits, subject to the limitations

described in the Government's letter, were admissible. *See* Cell Documents Decision. Pages from the Notebooks and the Malware Article, so redacted and with substitutions approved by the Court pursuant to CIPA § 6(c), were introduced at the prior trial. *See* Ex. G (GX801, from the Malware Article), H (GX806, from the Notebooks), I (GX809, from the Notebooks); Trial Tr. 334-35, 337-38, 339; *see also* Classified Dec. 19, 2019 Tr. at 45-78 & Classified Dec. 20, 2019 Tr. at 13-20 (discussing proposed exhibits from the MCC searches).

B. Relevant Law

The burden to establish that information is privileged unequivocally rests with the defendant. *See United States v. Schwimmer*, 892 F.2d 237, 244 (2d Cir. 1989). "To invoke the attorney-client privilege, a party must demonstrate that there was: (1) a communication between client and counsel, which (2) was intended to be and was in fact kept confidential, and (3) made for the purpose of obtaining or providing legal advice." *United States v. Constr. Prods. Research, Inc.*, 73 F.3d 464, 473 (2d Cir. 1996). Thus, the privilege does not attach to communications between two or more persons that do not enjoy an attorney-client relationship. *Schwimmer*, 892 F. 2d at 243 ("The relationship of attorney and client, a communication by the client relating to the subject matter upon which professional advice is sought, and the confidentiality of the expression for which the protection is claimed, all must be established in order for the privilege to attach."). Additionally, it is settled that even where an attorney-client relationship does exist, disclosure of a privileged communication to a third party waives privilege as to that communication. *See Schaeffler v. United States*, 806 F.3d 34, 40 (2d Cir. 2015) (privilege "is generally waived by voluntary disclosure of the [privileged] communication to another party").

To protect against the disclosure of attorney-client material during the execution of a search warrant, courts in this district have approved of a "common procedure" of designating a filter or wall team. *United States v. Ceglia*, No. 12 Cr. 876 (VSB), 2015 WL 1499194, at *1 (S.D.N.Y.

Mar. 8, 2015); *United States v. Feng Ling Liu*, No. 12 Cr. 934 (RA), 2014 WL 101672, at *11 (S.D.N.Y. Jan. 10, 2014); *see also United States v. Lumiere*, No. 16 Cr. 483 (JSR), 2016 WL 7188149, at *7 n. 10 (S.D.N.Y. Nov. 28, 2016) (noting that the Government proposed using a "'wall' protocol if it becomes aware of privileged documents . . . which may well moot [the defendant's suppression motion] entirely. "). The Government's use of a wall team is evidence of the Government's good faith. *See United States v. Patel*, No. 17 Cr. 798 (KBF), 2017 WL 3394607, at *7 (S.D.N.Y. Aug. 8, 2017) (the Government's use of a wall review team after identifying potentially privileged documents "do[es] not evidence the sort of bad faith or flagrant disregard of the warrant's limits that would justify the wholesale suppression of evidence"); *SEC v. Lek Secs. Corp.*, No. 17 Civ. 1789 (DLC) 2018 WL 417596, at *4 (S.D.N.Y. Jan. 16, 2018) (the SEC's use of a filter team "reflects respect for the privilege").

"[S]ince the attorney-client privilege stands in derogation of the public's right to every man's evidence, it ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle." *United States v. Jnt'l Bhd. Of Teamsters*, 119 F.3d 210, 214 (2d Cir. 1997) (ellipsis omitted). Even if law enforcement seizes privileged material alongside information responsive to the warrant, it is well settled that the proper remedy is suppression of the privileged material alone—not wholesale suppression of the entire search. *See, e.g., Nat'l City Trading Corp. v. United States*, 635 F.2d 1020, 1026 (2d Cir. 1980) (in the context of a search of a law office pursuant to a search warrant, "[t]o the extent that the files obtained here were privileged, the remedy is suppression and return of the documents in question, not invalidation of the search" (citation omitted)); *Patel*, 2017 WL 3394607, at *6 ("'The general remedy for violation of the attorney-client privilege is to suppress introduction of the privileged information at trial,' not to order wholesale suppression." (quoting *Lumiere*, 2016 WL 7188149, at *6)); *Feng Ling Liu*, 2014

WL 101672, at *11 (same); *United States v. Chuang*, 696 F. Supp. 910, 915 (S.D.N.Y. 1988) (same); *United States v. Giovanelli*, 747 F. Supp. 891, 894 (S.D.N.Y. 1989) (refusing to suppress the entirety of a notebook seized by the Government where at least portions of the notebook were properly seized). "[T]he drastic remedy of the suppression of all evidence seized is not justified unless those executing the warrant acted in flagrant disregard of the warrant's terms." *United States v. Matias*, 836 F.2d 744, 747-48 (2d Cir. 1988) (citing cases); *see also Kaplan*, 2003 WL 22880914, at *11 (suppressing evidence where law enforcement disregarded court-ordered procedures, including by allowing the case agent, rather than the wall-team prosecutors, to determine if crime-fraud exception applied).

C. Argument

As with the other relief sought in the Motion, the defendant identifies no "intervening change of controlling law," no "availability of new evidence," and identifies no "clear error" in the Court's prior ruling denying his motion to suppress evidence obtained from the MCC searches and receiving GX801, 806, and 809 into evidence. *Bush*, 2021 WL 371782, at *1. Accordingly, the Court should not reconsider its prior rulings with respect to these exhibits. Moreover, the defendant's current privilege assertions over particular portions of GX801, 806, and 809 are contradicted by his earlier failure to assert them and by the exhibits' admission into evidence at his public trial.

The defendant argues that objections to GX801, 806, and 809 based on alleged privilege have not previously been litigated, Mot. 55-56, but he omits any reference to letters filed by the Government and by his counsel addressing these specific documents, D.E. 257, 282, 285; and the Court's Cell Documents Decision. The defendant's motion to suppress is a request to reconsider the Court's prior rulings denying suppression, and finding the admissibility, of GX801, 806, and 809, and the defendant must meet the standards for reconsideration. That he has failed to do.

The defendant generally argues that the MCC Premises Warrant only permitted the search for and seizure of "nine identified titles," *see, e.g.*, Mot. 57, 61, 62, 64 & 65; and that the Malware Article and Notebooks were outside the scope of the warrant. This contention is incorrect and already has been rejected by the Court: "The terms of the warrant here included the following description to be seized: '[a]ny and all notes, documents, records, correspondence, or materials, in any format and medium . . . pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents and materials[.]" MCC Suppression Dec. at 5. "Thus, to the extent the notebooks found in Schulte's cell contained relevant evidence they are undoubtedly in the scope of the warrant." *Id.*

The defendant next attempts to argue that GX801, 806, and 809 are privileged, but his efforts fail to carry his burden of showing the documents constitute "(1) a communication between client and counsel, which (2) was intended to be and was in fact kept confidential, and (3) made for the purpose of obtaining or providing legal advice." *Constr. Prods. Research, Inc.*, 73 F.3d at 473. Indeed, his arguments are contradicted by the contents of the documents themselves and other evidence showing the defendant's intent to use or disclose the contents of the documents for extra-legal purposes.

The defendant argues at length that the Malware Article is privileged because it was prepared "exclusively for his attorneys" and he "only ever shared it with them, for the sole purpose of his defense." Mot. 56 & 57-61. But (1) the defendant did not assert privilege over the Malware Article in his January 27, 2020 letter challenging the admissibility of the selected documents from the MCC search (D.E. 281 at 5);[12] and (2) the Malware Article is addressed "To my fellow

[12] The defendant asserted privilege over limited portions of a second version of the Malware Article, but not over the version introduced as GX801. *Compare* D.E. 257 at 12 & 13-14 (describing the "Identifying Malware of the Mind as Article 10" and "The Malware Article

engineers and the tech industry," Ex. G at 2, plainly evincing his intent that the document would not be confidential. The defendant also admits that he continued editing the Malware Article expressly for the purpose of publication, *see* Mot. 58; and had caused nine other "articles" to be published on the internet. *See also* Ex. I at 3 (the defendant describing his plans to publish 10 articles on Wordpress and Facebook). The defendant's self-serving and unsubstantiated claim that he intended the document from which GX801 is derived as an attorney-client communication solely for the purpose of obtaining legal advice is conclusory and fails to explain how the article was in furtherance of his defense or obtaining legal advice; and is flatly contradicted by the content of the document, his prior failure to assert privilege over the document, and his admitted ongoing efforts to publish a version of that document.

The defendant also argues that other portions of GX806 and 809 are privileged,[13] including (i) lists of encrypted and anonymous email facilities the defendant created and operated from the MCC using the contraband cellphones and their passwords, Mot. 62; (ii) the defendant's statement that "[i]f govt doesn't pay me $50 billion in restitution and prosecute the criminals who lied to the judge and presented this BS case" he would work to harm U.S. foreign policy (with the strong inference that he intended to do so by disclosing classified information), *id.* 62-63; (iii) the defendant's statement about waging an "information war" against the United States, *id.* 63-34; (iv) the defendant's statements about how he developed file partition tools for classified operations and "if you need help ask WikiLeaks for my code," *id.* 64; and (iv) the defendant's "decision to publicly release an unclassified redress of grievances," *id.* 65. The defendant fails to carry his

---

(undated)" *with* D.E. 282 at 5 (asserting privilege over specific portions of "Identifying Malware of the Mind as Article 10").

[13] The defendant's page cites to GX806 and 809 at times do not correspond to the materials he appears to reference.

burden of establishing privilege for any of these passages. He did not assert privilege over these portions of the Notebooks when they were identified as proposed Government exhibits. *See* D.E. 282. And he offers no explanation now of how the statements were in furtherance of his legal defense or for obtaining legal advice. The identification of anonymous email accounts and their passwords is, on its face, not for the purpose of obtaining legal advice, particularly where the defendant used those accounts to transmit classified material and material covered by protective order. The defendant's threat to disrupt foreign relations if he didn't get a $50 billion payout similarly has nothing to do with a legal defense or with obtaining legal advice. With respect to the defendant's "information war," he admits that he carried out aspects of that war "with assistance from his family"—that is, non-confidentially and outside the confines of the attorney-client relationship, *see, e.g., United States v. Stewart*, 287 F. Supp. 2d 461, 464 (S.D.N.Y. 2003) (disclosing attorney-client communication to client's daughter waived privilege), and that it was a publicity campaign rather than a legal strategy. The same is true for his "decision to publicly release an unclassified redress of grievances"—the defendant's intention that the communication would not be confidential precludes the application of the privilege. The defendant's discussion of classified cyber operations using file partition tools that he developed similarly bears no logical relation to legal advice or his legal defense strategy.

There is no indication, other than the defendant's conclusory and unsubstantiated assertions, that any these statements were intended as confidential communications to the defendant's attorneys or were for the purpose of obtaining legal advice and, to the contrary, they are plainly non-legal in character and evince the defendant's intent to communicate with third parties and the public. And even if the defendant had communicated these statements to his counsel or had intended to do so, "a document is not privileged merely because it was sent or received

between an attorney and client, it must contain confidential communication relating to legal advice." *United States v. Correia*, 468 F. Supp. 3d 618, 622 (S.D.N.Y. 2020) (cleaned up). Moreover, communications with an attorney are not protected by the privilege if they are in furtherance of contemplated or ongoing criminal or fraudulent conduct, *In re Grand Jury Subpoena Duces Tecum*, 731 F.2d 1032, 1038 (2d Cir. 1984), as the defendant's extortionate threats and campaign to disclose classified and protected documents appear to be.

The defendant fails to satisfy the standard for reconsideration of the Court's prior orders denying suppression of GX801, 806, and 809 and admitting them into evidence at trial; the defendant failed to assert privilege over the unredacted portions of those exhibits in connection with prior litigation over admissibility and privilege claims; and his recent assertion of privilege is conclusory and contradicted by the statements, their context, and his own admissions showing the absence of confidentiality and purposes unrelated to legal advice. The defendant's motion to suppress should be denied.

CONCLUSION

For the foregoing reasons, the defendant's motions should be denied.

Dated: New York, New York
February 25, 2022

DAMIAN WILLIAMS
United States Attorney

By: /s/
David W. Denton, Jr. / Michael D. Lockard
Assistant United States Attorneys
(212) 637-2744 / -2193